UNITED STATES PATENT AND TRADEMARK OFFICE

NOTICE OF ALLOWANCE AND FEE(S) DUE

21552   7590   11/03/2010

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
SALT LAKE CITY, UT 84101

EXAMINER
BROWN, CHRISTOPHER J

ART UNIT	PAPER NUMBER
2439	

DATE MAILED: 11/03/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,714	12/21/2001	David M. Austin	AUZ-002 P	6090

TITLE OF INVENTION: DETECTION OF OBSERVERS AND COUNTERMEASURES AGAINST OBSERVERS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$0	$0	$755	02/03/2011

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: <u>Mail</u>

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or <u>Fax</u> (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

21552   7590   11/03/2010

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
SALT LAKE CITY, UT 84101

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

_____ (Depositor's name)

_____ (Signature)

_____ (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,714	12/21/2001	David M. Austin	AUZ-002 P	6090

TITLE OF INVENTION: DETECTION OF OBSERVERS AND COUNTERMEASURES AGAINST OBSERVERS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$0	$0	$755	02/03/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
BROWN, CHRISTOPHER J	2439	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE   (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____   Date _____

Typed or printed name _____   Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,714	12/21/2001	David M. Austin	AUZ-002 P	6090

			EXAMINER
21552	7590	11/03/2010	BROWN, CHRISTOPHER J

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
SALT LAKE CITY, UT 84101

ART UNIT	PAPER NUMBER
2439	

DATE MAILED: 11/03/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 798 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 798 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101   or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

	Application No.	Applicant(s)
Notice of Allowability	10/027,714	AUSTIN ET AL.
	Examiner	Art Unit	
	CHRISTOPHER J. BROWN	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/24/2010*.

2. ☒ The allowed claim(s) is/are *1-18,20 and 21*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the

            International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

        Paper No./Mail Date _____.

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08),
    Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☐ Interview Summary (PTO-413),
    Paper No./Mail Date _____ .

7. ☒ Examiner's Amendment/Comment

8. ☐ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____.

/Christopher J Brown/
Primary Examiner, Art Unit 2439

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Wes Austin on 10/27/2010.

REPLACE the current claims with the following:

1. A computer program embodied in a non-transitory computer-readable medium for scanning a computer for observer programs, the computer program comprising:

   observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data, and wherein the log data includes screen shots, program usage and web sites visited;

   reading instructions that read memory of the computer to obtain memory data;

   comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;

   generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer;

   countermeasure instructions that alter the operation of the observer program;

   outputting instructions that provide the results through a graphical user interface and that prompt as to whether the countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running;

   disabling instructions to disable the observer program if it is present on the computer, the disabling instructions implementing a method comprising:

   entering a startup command to load a kill program before the observer program is started;

   rebooting the computer;

   starting the kill program by execution of the startup command; and

   deleting an observer program startup command so that the observer program is not started.

2. The computer program of claim 1 wherein the memory data includes startup commands.

3. The computer program of claim 1 wherein the memory data includes registry startup commands.

4. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer import table data and wherein the comparing instructions compare memory import table data from the memory data characteristics with the observer import table data to determine whether an observer program is present on the computer.

5. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer export table data and wherein the comparing instructions compare memory export table data from the memory data characteristics with the observer export table data to determine whether an observer program is present on the computer.

6. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer resource data and wherein the comparing instructions compare memory resource data from the memory data characteristics with the observer resource data to determine whether an observer program is present on the computer.

7. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer file content data and wherein the comparing instructions compare memory file content data from the memory data characteristics with the observer file content data to determine whether an observer program is present on the computer.

8. The computer program of claim 7 wherein the comparing instructions compare the observer file content data with the memory file content data at an offset address.

9. The computer program of claim 7 wherein the comparing instructions compare the observer file content data with a span of the memory file content identified by an offset address.

10. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer module loading data and wherein the comparing instructions compare memory module loading data from the memory data characteristics with the observer module loading data to determine whether an observer program is present on the computer.

11. The computer program of claim 1 wherein the plurality of observer program characteristics includes OS observing functions and wherein the comparing instructions compare memory functions from the memory data characteristics with the OS observing functions to determine whether an observer program is present on the computer.

12. The computer program of claim 1 wherein the memory data includes explorer extension data.

13. The computer program of claim 1 wherein the memory data includes file use information.

14. The computer program of claim 1 wherein the memory data includes process information.

15. The computer program of claim 1 wherein the memory data includes running process information.

16. The computer program of claim 1 wherein the memory data includes loaded modules information.

17. The computer program of claim 1 wherein the memory data includes driver data.

18. The computer program of claim 1 wherein the memory data includes kernel driver data.

19. (Canceled)

20. The computer program of claim [[19]] 1 wherein the method further comprises deleting
    observer program files.

21. A method embodied in a non-transitory computer-readable medium for scanning a computer
for observer programs, the method comprising:

   using observer data comprising a plurality of observer program characteristics descriptive of
        a plurality of observer programs where the observer programs are programmed to
        observe activities on a computer system and to create log data, and wherein the log
        data includes screen shots, program usage and web sites visited;

   reading memory of the computer to obtain memory data;

   comparing the plurality of observer program characteristics with memory data characteristics
        to determine whether an observer program is present on the computer;

   generating results from the comparing, wherein the results generated indicate whether the
        observer program is present on the computer;

   outputting the results through a graphical user interface; and

   prompting the user as to whether countermeasure instructions should be executed, wherein
        the countermeasure instructions are executable to (1) temporarily disable the observer
        program, (2) permanently disable the observer program, and (3) create decoy
        observer created data but wherein the observer program continues running;

   disabling instructions to disable the observer program if it is present on the computer, the
        disabling instructions implementing a method comprising:

                entering a startup command to load a kill program before the observer
                    program is started;

                rebooting the computer;

                starting the kill program by execution of the startup command; and

                deleting an observer program startup command so that the observer program
                    is not started.

   .

22-34. (Canceled)

Allowable Subject Matter

Claims 1-18, 20-21 allowed. Claims are allowable over the current art of record due to applicants amendments and persuasive arguments. Claim limitations are enough that motivation to combine would not have been sufficient.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/   10/28/2010
Primary Examiner, Art Unit 2439